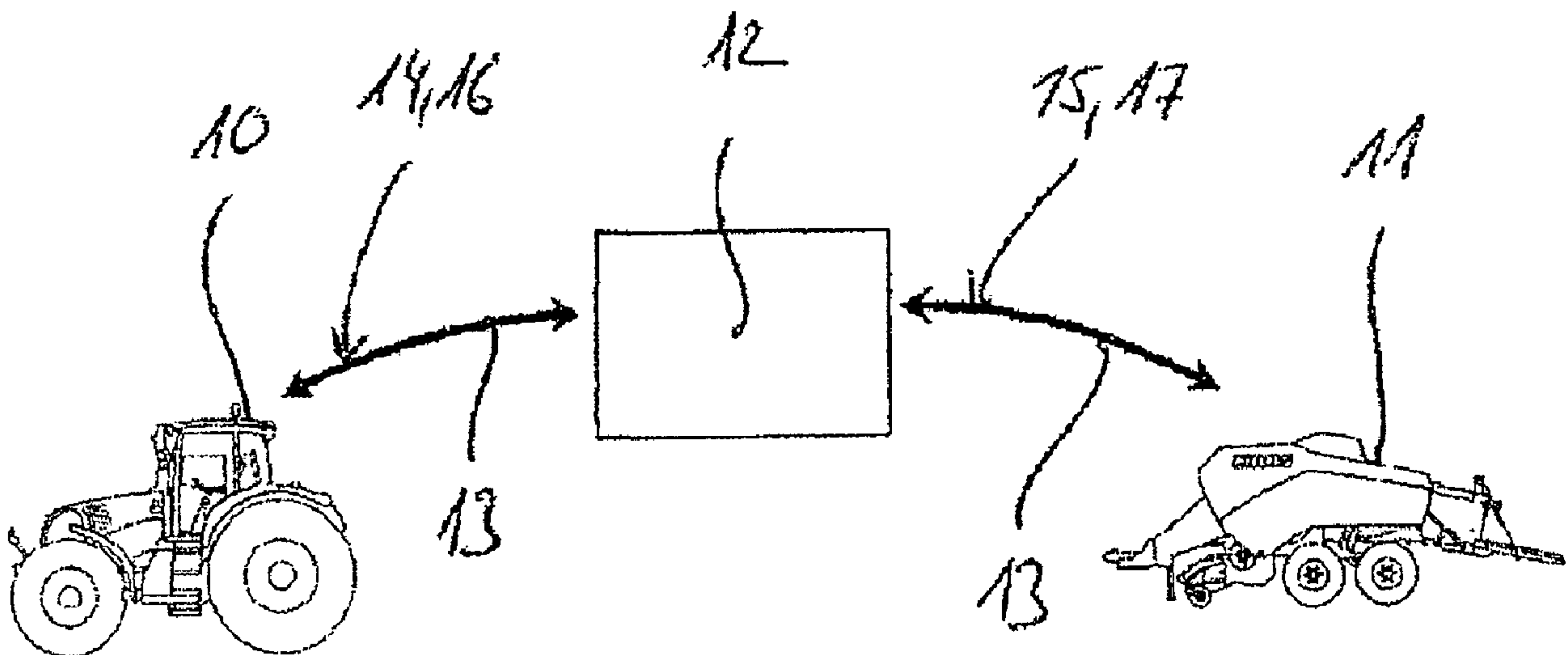




(22) Date de dépôt/Filing Date: 2013/12/19
(41) Mise à la disp. pub./Open to Public Insp.: 2014/07/08
(45) Date de délivrance/Issue Date: 2016/01/26
(30) Priorité/Priority: 2013/01/08 (DE102013000088.2)

(51) Cl.Int./Int.Cl. *A01D 75/00* (2006.01),
G07C 11/00 (2006.01)
(72) Inventeurs/Inventors:
JENINGA, JASPER, DE;
DIRLEWANGER, FLORIAN, DE;
MOCK, ANDREAS, DE
(73) Propriétaire/Owner:
CLAAS E-SYSTEMS KGAA MBH & CO KG, DE
(74) Agent: KIRBY EADES GALE BAKER

(54) Titre : PROCEDE ET APPAREIL DESTINES A L'AUTHENTIFICATION D'AU MOINS DEUX MACHINES AGRICOLES
COUPLEES PAR LE BIAIS D'UN BUS DE DONNEES
(54) Title: METHOD AND APPARATUS FOR AUTHENTICATING AT LEAST TWO AGRICULTURAL MACHINES
COUPLED VIA A DATA BUS



(57) Abrégé/Abstract:

A method for authenticating at least two agricultural machines coupled via a data bus, comprising the following steps: each of the agricultural machines coupled with the data bus is subjected, automatically and independently of the or any other agricultural device, to an authentication process by an authentication device, which is also coupled with the data bus; subsequently, a direct data exchange or indirect data exchange is automatically enabled between the successfully authenticated agricultural machines, while any data exchange with an agricultural machine that has not been successfully authenticated is disabled.



ABSTRACT

A method for authenticating at least two agricultural machines coupled via a data
5 bus, comprising the following steps: each of the agricultural machines coupled
with the data bus is subjected, automatically and independently of the or any
other agricultural device, to an authentication process by an authentication
device, which is also coupled with the data bus; subsequently, a direct data
exchange or indirect data exchange is automatically enabled between the
10 successfully authenticated agricultural machines, while any data exchange with
an agricultural machine that has not been successfully authenticated is disabled.

**METHOD AND APPARATUS FOR AUTHENTICATING AT LEAST TWO
AGRICULTURAL MACHINES COUPLED VIA A DATA BUS**

5

FIELD AND BACKGROUND

This invention relates to a method for authenticating at least two agricultural machines coupled via a data bus. Furthermore, the invention relates to an authentication device for implementing the method.

10 In order to perform certain agricultural operations, it is necessary to couple at least two agricultural devices mechanically and/or hydraulically and/or pneumatically and/or electrically. In order to run harvesting operations, it may be necessary to couple a first agricultural machine, designed as a tractor, with a second agricultural machine, designed as a harvester. In doing so, the harvester is driven by the

15 tractor, which provides mechanical power and/or hydraulic power and/or pneumatic power and/or electrical power to operate the harvester. In addition, modern agricultural equipment can be coupled on the control side via a data bus in order to facilitate an exchange of control-side data. For example, the design may provide for the harvester to influence the operation of the tractor; for example, the harvester

20 may request more power from the tractor and/or influence the tractor's direction of movement. In doing so, it must be ensured that any influence on the operation of the tractor by the harvester does not result in any unsafe operating mode for the tractor. Similarly, the tractor must not cause any unsafe operating mode for the harvester. Therefore, only properly licensed or certified agricultural machines should

25 be coupled on the control side. This can be ensured by authenticating the agricultural devices coupled via the data bus.

It is known from previous practical applications that agricultural devices coupled via a data bus can be authenticated by the operator of the devices accessing and/or entering authentication codes via the Internet or via mobile phone. Such methods require input from the operator, making the authentication process prone to error. In
5 some cases, there may also be limited or no Internet or mobile phone access so that no authentication is possible.

Based on this premise, the object of the present invention is to provide a novel method for authenticating at least two agricultural machines coupled via a data bus, as well as an authentication device for implementing the method.

10 SUMMARY

Certain exemplary embodiments can provide a method for authenticating of at least two agricultural devices coupled via a data bus prior to implementing data exchange therebetween, comprising the steps of: coupling an authentication device and the at least two agricultural devices to the data bus; utilizing the authentication device to
15 authenticate each of the at least two agricultural devices coupled to the data bus automatically and independently; upon successful authentication of the at least two agricultural devices, implementing direct data exchange or indirect data exchange between the successfully authenticated agricultural devices, automatically; and upon unsuccessful authentication, blocking direct data exchange or indirect data exchange
20 between the unsuccessfully authenticated agricultural devices.

Certain exemplary embodiments can also provide an authentication device configured for authenticating at least two agricultural devices coupled via a data bus prior to implementing data exchange therebetween, utilizing a method comprising the steps of: coupling an authentication device and the at least two agricultural devices to
25 the data bus; utilizing the authentication device to authenticate each of the at least two agricultural devices coupled to the data bus automatically and independently; upon successful authentication of the at least two agricultural devices, implementing direct data exchange or indirect data exchange between the successfully

2a

authenticated agricultural devices, automatically; and upon unsuccessful authentication, blocking direct data exchange or indirect data exchange between the unsuccessfully authenticated agricultural devices.

Further exemplary embodiments can provide a computer program product
5 comprising program code means embodied in a non-transitory computer readable medium for carrying out all steps of a method for authenticating of at least two agricultural devices coupled via a data bus prior to implementing data exchange therebetween, when the program code means is run on a computer or control device, the method comprising the steps of: coupling an authentication device and the at
10 least two agricultural devices to the data bus; utilizing the authentication device to authenticate each of the at least two agricultural devices coupled to the data bus automatically and independently; upon successful authentication of the at least two agricultural devices, implementing direct data exchange or indirect data exchange between the successfully authenticated agricultural devices, automatically; and upon
15 unsuccessful authentication, blocking direct data exchange or indirect data exchange between the unsuccessfully authenticated agricultural devices.

According to the invention, the authentication of at least two agricultural machines coupled via a data bus is achieved via the following steps: Each of the agricultural machines coupled to the data bus is subjected, automatically and independently of the
20 or any other agricultural device, to an authentication process via an authentication device, which is also coupled with the data bus; subsequently, a direct or indirect exchange of data is automatically enabled between the successfully authenticated agricultural machines, while any data exchange with an agricultural machine that has

not been successfully authenticated is automatically disabled. The authentication method according to the invention is a fully automated process that requires no input from the operator. No Internet or mobile phone access is required.

According to an advantageous further development of the invention, the authentication
5 of each agricultural machine coupled with the data bus involves, on the one hand, the authentication device being verified via the individual agricultural machine and, on the other hand, the individual agricultural machine being verified via the authentication device, respectively. This authentication process is fully automated and is bug-proof.

Preferably, the verification of the authentication device via the individual agricultural
10 machine should be achieved via the following steps: the individual agricultural machine transmits an identification code stored in its control unit and a random number generated by its control unit to the authentication device; the authentication device calculates a first device key from the identification number transmitted by the individual agricultural machine; the authentication device calculates a second device
15 key from the first device key and the random number transmitted by the individual agricultural machine; the authentication device transmits the second device key and a random number generated by the authentication device to the control unit of the individual agricultural machine; the individual agricultural machine also calculates a second device key from the first device key stored in its control unit and the random
20 number generated by the control unit and then compares this second device key calculated by its control unit to the second device key calculated and transmitted by the authentication device. Then, if these two second device keys match, the authentication device has been successfully verified via the individual agricultural machine.

25 Preferably, the verification of the individual agricultural machine via the authentication device should be achieved via the following steps: the individual agricultural machine calculates a third device key from the first device key stored in its control unit and from the random number transmitted by the authentication device

and then transmits that third device key to the authentication device; the authentication device also calculates a third device key from the first device key and the random number, which it calculated and then compares that third device key to the third device key calculated and transmitted by the individual agricultural machine. Then, if the two third device keys match, the individual agricultural machine has been successfully verified via the authentication device.

Neither the authentication device verification process described above nor the agricultural machine verification process described above involve the transmission of any secret device keys of the individual agricultural machine, but rather exclusively involve the transmission of randomly generated numbers and non-reversibly calculated device keys based on these random numbers. The authentication process according to the invention is therefore bug-proof.

Upon successful verification of the authentication device and the individual agricultural machine, the individual agricultural machine is successfully authenticated. Subsequently, a direct data exchange or indirect data exchange is automatically enabled between the successfully authenticated agricultural machines. An indirect exchange of data between successfully authenticated agricultural machines is performed via the authentication device. A direct exchange of data between successfully authenticated agricultural machines is implemented via circumvention of the authentication device, in particular via combination keys generated specifically for this purpose.

BRIEF DESCRIPTION OF THE DRAWINGS

Preferred further developments of the invention are apparent from the dependent claims and the description below. Illustrative embodiments of the invention including, but not limited to, those shown in the drawings, are explained below. The drawings show:

Fig. 1 a first schematic diagram of two agricultural machines coupled via a data bus, illustrating a first variant of the invention;

Fig. 2 a second schematic diagram of two agricultural machines coupled via a data bus, illustrating a second variant of the invention;

Fig. 3 a signal flow diagram illustrating the authentication of the agricultural machines coupled via the data bus; and

Fig. 4 a signal flow diagram illustrating the calculation of combination keys for use in a direct exchange of data between successfully authenticated agricultural machines.

DETAILED DESCRIPTION

The invention relates to a method of authenticating at least two agricultural machines coupled via a data bus. Furthermore, the invention relates to an authentication device for implementing the method.

Described below is an application of the invention in which a first agricultural machine designed as a tractor by a first manufacturer is to be coupled on the control side via a data bus with a second agricultural machine designed as a harvester by a different, second manufacturer.

The invention, however, is not limited to this application. In fact, the invention can be used whenever two agricultural machines, typically made by different manufacturers, need to be coupled.

The authentication of the two agricultural machines and, i.e. the tractor and the harvester is achieved via the following steps: first, each of the agricultural machines coupled with the data bus is subjected, automatically and independently of the or any other agricultural device, to an authentication process by an authentication

device which is also coupled with the data bus. Subsequently, an indirect data exchange (see Fig. 1) or a direct data exchange (see Fig. 2) is automatically enabled between the successfully authenticated agricultural machines, while any data exchange with an agricultural machine that has not been successfully authenticated is automatically disabled.

This invention ensures, in a fully automated process not requiring any input from the operator and not necessitating any Internet or mobile phone access, that only properly licensed and/or certified agricultural machines can be coupled together on the control side. Thereby, it also ensures via a fully automated process that only properly licensed and/or certified agricultural machines are combined to operate together and influence each others' operations.

The authentication of each agricultural machine coupled with the data bus involves, on the one hand, the authentication device being verified via the individual agricultural machine and, on the other hand, the individual agricultural machine being verified via the authentication device, respectively. This is described in detail below, with reference to Fig. 3.

Block 19 illustrates how an identification code ID-LGi ($i=10, 11$) of each individual agricultural machine and a secret, first device key KEY-LGi are stored in the individual agricultural machine, specifically in a control unit of the said machine. As shown in block 20, the individual agricultural machine, specifically its control unit, generates a random number. The individual agricultural machine transmits the identification code ID-LGi stored in its control unit, as well as the random number generated by the control unit, to the authentication device via the data bus. The secret, first device key KEY-LGi of the individual agricultural machine is not transmitted. As shown in block 21, the authentication device uses the identification code ID-LGi transmitted by the individual agricultural machine to calculate a first device key KEY1-A-LGi, using a key generator implemented in the authentication device. As shown in block 22, the authentication device uses the first device key

KEY1-A-LG1 and the random number transmitted by the individual agricultural machine to calculate a second device key KEY2-A-LGi. The authentication device also generates a random number. The authentication device transmits the second device key KEY2-A-LGi and the random number generated by the authentication device to the control unit of the individual agricultural device via the data bus. As seen in block 24, the individual agricultural machine also calculates a second device key KEY2-LGi from the first, secret device key KEY1-LGi stored in the control unit of the agricultural machine and the random number generated by the control unit. In a block 25, the individual agricultural machine compares the second device key KEY2-LGi, which it calculated to the second device key KEY2-A-LG1 calculated and transmitted by the authentication device. Then, if the two second device keys KEY2-A-LGi and KEY2-LGi match, the authentication device has been successfully verified by the individual agricultural machine, and it is branched off to block 27. However, if the two second device keys KEY2-A-LGi and KEY2-LGi do not match, the authentication device has not been successfully verified, and it is branched off to block 26, the authentication process then being terminated as unsuccessful in block 26.

In block 27, the individual agricultural machine calculates a third device key KEY3-LGi from the first device key KEY1-LGi stored in its control unit and from the random number transmitted by the authentication device. The individual agricultural machine then transmits this third device key KEY3-LGi to the authentication device via the data bus. In block 28, the authentication device uses the first device key KEY1-A-LGi, which it calculated and the random number, which it generated to calculate a third device key KEY3-A-LGi, as well. As seen in block 29, the authentication device then compares the third device key KEY3-A-LGi calculated by the authentication device to the third device key KEY3-LGi calculated and transmitted by the individual agricultural machine. Then, if the two third device keys KEY3-A-LGi and KEY3-LGi match, the individual agricultural machine has been successfully verified by the authentication device. However, if the two third device keys KEY3-A-LGi and KEY3-

LG_i do not match, the individual agricultural machine has not been successfully verified and is branched off to block 30, the authentication process then being terminated as unsuccessful in block 30.

In the preferred application involving the coupling of a first individual agricultural machine designed as a tractor and a second individual agricultural machine designed as a harvester, the authentication of the tractor and the harvester takes place independently of each other, preferably as described below:

As seen in block 19, an identification code ID-LG10 of the tractor and a secret first device key KEY-LG10 of the tractor are stored in the control unit of the tractor. As shown in block 20, the tractor generates a random number. The tractor transmits the identification code ID-LG10 stored in its control unit and the random number generated by the control unit to the authentication device via the data bus. In doing so, the secret first device key KEY-LG10 of the tractor is not transmitted.

As shown in block 21, the authentication device uses the identification code ID-LG10 transmitted by the tractor to calculate a first device key KEY1-A-LG10 of the tractor, using a key generator implemented in the authentication device. The authentication device uses the first device key KEY1-A-LG10 and the random number transmitted by the tractor to calculate a second device key KEY2-A-LG10 of the tractor, as shown in block 22. The authentication device also generates a random number. The authentication device transmits the second device key KEY2-A-LG10 and the random number generated by the authentication device to the control unit of the tractor via the data bus. As shown in block 24, the tractor then uses the first, secret device key KEY1-LG10 stored in its control unit and the random number generated by the control unit to calculate a second device key KEY2-LG10 of the tractor, as well. In block 25, the tractor compares the second device key KEY2-LG10 calculated by its control unit to the second device key KEY2-A-LG10 of the tractor transmitted by the authentication device. Then, if the two second device keys KEY2-A-LG10 and KEY2-LG10 match, the authentication device has been

successfully verified by the tractor. In this case, i.e. upon successful verification of the authentication device, the tractor uses the first secret device key KEY1-LG10 stored in its control unit and the random number transmitted by the authentication device to calculate a third device key KEY3-LG10 for the tractor. The tractor then
5 transmits this third device key KEY3-LG10 to the authentication device via the data bus. In block 28, the authentication device uses the first device key KEY1-A-LG10, which it calculated and the random number, which it generated to calculate a third device key KEY3-A-LG10 for the tractor, as well. As shown in block 29, the authentication device then compares the two third device keys KEY3-A-LG10 and
10 KEY3-LG10. Then, if the two third device keys match, the tractor has been successfully verified by the authentication device. Upon successful verification of the authentication device via the tractor and successful verification of the tractor via the authentication device, the authentication process of the tractor is successfully completed.

15 The authentication of the harvester is implemented analogously: As shown in block 19, an identification code ID-LG11 of the harvester and a secret first device key KEY-LG11 of the harvester are stored in the harvester. As shown in block 20, the harvester generates a random number. The harvester transmits the identification code ID-LG11 stored inside it and the random number generated by it to the
20 authentication device via the data bus. The secret first device key KEY-LG11 of the harvester is not transferred. As shown in block 21, the authentication device uses the identification code ID-LG11 transmitted by the harvester to calculate a first device key KEY1-A-LG11 of the harvester, using a key generator implemented in the authentication device. The authentication device uses the first device key KEY1-
25 A-LG11 and the random number transmitted by the harvester to calculate a second device key KEY2-A-LG11 of the harvester, as shown in block 22. The authentication device also generates a random number. The authentication device transmits the second device key KEY2-A-LG11 of the harvester and the random number generated by the authentication device to the harvester via the data bus. As shown

in block 24, the harvester uses the secret first device key KEY1-LG11 stored inside it and the random number generated by it to calculate a second device key KEY2-LG11 of the harvester, as well. In block 25, the harvester compares the second device key KEY2-LG11, which it calculated to the second device key KEY2-A-LG11 of the harvester transmitted by the authentication device. Then, if the two second device keys KEY2-A-LG11 and KEY2-LG11 match, the authentication device has been successfully verified by the harvester. In this case, the harvester uses the secret first device key KEY1-LG11 and the random number transmitted by the authentication device to calculate a third device key KEY3-LG11. The harvester then transmits this third device key KEY3-LGi to the authentication device via the data bus. In block 28, the authentication device uses the first device key KEY1-A-LG11, which it calculated and the random number, which it generated to calculate a third device key KEY3-A-LG11 for the harvester, as well. As shown in block 29, the authentication device then compares the two third device keys KEY3-A-LG11 and KEY3-LG11. Then, if the two third device keys match, the harvester has been successfully verified by the authentication device. Upon successful verification of the authentication device by the harvester and upon successful verification of the harvester by the authentication device, the authentication process of the harvester is successfully completed.

It should be noted at this point that the secret first device key KEY1-LGi ($i=10, 11$) stored in the individual agricultural machine and the first device key KEY1-A-LGi calculated by the authentication device are calculated for the individual agricultural device/machine using the same key generators. In doing so, the secret first device key KEY1-LGi stored in the agricultural machine is calculated via a key generator of an independent superordinate database. The first device key KEY1-A-LGi is calculated inside the authentication device by a key generator of the same type implemented in the authentication device. It should also be noted at this point that at least the calculation of the second device key KEY2-A-LGi in block 22 by the authentication device and the calculation of the third device key KEY3-LGi in block

27 by the individual agricultural device are implemented by means of a non-reversible calculation method, such as a CRC32 calculation method. This ensures that the device keys KEY2-A-LGi and KEY3-LGi transmitted via the data bus cannot be used to reverse-calculate the secret device key KEY1-LGi ($i=10, 11$) of the
5 individual agricultural machine. This method increases the bug-proof property of the method according to the invention.

Subsequently, if an indirect exchange of data is to take place between the tractor and the harvester via the authentication device, as shown in Fig. 1, the successful authentication of the tractor and harvester subsequently automatically enables a
10 data exchange between the successfully authenticated tractor and the successfully authenticated harvester via the authentication device.

Subsequently, if a direct exchange of data is to take place between the tractor and harvester while circumventing the authentication device, as shown in Fig. 2, the successful authentication of the tractor and harvester subsequently requires the
15 calculation of combination keys, which are then used to enable a direct data exchange. This is described in detail below, with reference to Fig. 4.

As shown in Fig. 4, the authentication device, in order to enable a direct data exchange between the first agricultural machine, preferably designed as a tractor, and the second agricultural machine, preferably designed as a harvester, uses an
20 additional random number generated by the authentication device in block 31 and a first device key KEY1-A-LG10 calculated for the first agricultural machine by the authentication device in block 21 in order to calculate a fourth device key KEY4-A-LG10 for the first agricultural machine, as shown in block 32. As seen in block 33, the authentication device also calculates a secret combination key KEYC-A, this
25 secret combination key KEYC-A particularly being a random number. In block 34, the authentication device uses the first device key KEY1-A-LG10 calculated in block 21, the fourth device key KEY4-A-LG10 calculated in block 32, and the combination key KEYC-A calculated in block 32 to calculate a system key KEYC-A-LG10 for the

first agricultural machine. The authentication device then transmits this system key KEYC-A-LG10, as well as the additional random number, to the first agricultural machine; in doing so, the first agricultural machine uses the system key KEYC-A-LG10 and the additional random number to calculate the combination key KEYC in a block 35. The system key KEYC-A-LG10 transmitted by the authentication device and the additional random number can be used to reverse-calculate the combination key KEYC, but not the secret first device key KEY1-LG10. The first agricultural machine stores the combination key KEYC and uses it for a subsequent encrypted data exchange with the second agricultural machine.

As can also be seen in Fig. 4, that the authentication device, in block 37, subsequently uses an additional random number, which it generated in block, as well as the first device key KEY1-A-LG11, which it calculated for the second agricultural machine in block 21, to calculate a fourth device key KEY4-A-LG11 for the second agricultural machine. In block 38, the authentication device then uses the first device key KEY1-A-LG11 calculated in block 21, the fourth device key KEY4-A-LG11 calculated in block 37, and the combination key KEYC-A calculated in block 33 to calculate a system key KEYC-A-LG11 for the second agricultural machine. The authentication device then transmits the system key KEYC-A-LG11, as well as the additional random number, to the second agricultural machine; in doing so, the second agricultural machine uses the system key KEYC-A-LG11 and the additional random number to calculate the combination key KEYC in a block 39. The system key KEYC-A-LG11 transmitted by the authentication device and the additional random number can be used to reverse-calculate the combination key KEYC, but not the secret first device key KEY1-LG11 of the second agricultural machine. The second agricultural machine stores the combination key KEYC and uses it for a subsequent encrypted data exchange with the first agricultural machine.

A subsequent direct, encrypted data exchange between the two agricultural machines is implemented using the combination key KEYC.

The authentication device according to the invention comprises the means for implementing the method according to the invention; at least the means for implementing the authentication process as described in blocks 19 to 30 and, in the case of a direct data exchange between the authenticated agricultural machines, additional means for implementing blocks 31 to 39. These means comprise at least one interface for the data exchange between the agricultural machines and; a memory for storing the relevant data; and a processor for calculating the relevant data.

The authentication device can be designed as an independent assembly or as an integrated part of the control units of the agricultural machines and. For example, one option is to design the authentication device as a USB stick that can be coupled with the data bus via a USB interface in one of the agricultural machines.

In all of the embodiments described, the preferred data bus is a so-called ISOBUS. This is a CAN bus standardized to ISO 11783, which regulates communication between agricultural machinery, including, in particular, communication between agricultural machines made by different manufacturers.

List of reference signs

	10	agricultural machine
	11	agricultural machine
	12	authentication device
5	13	data bus
	14	authentication
	15	authentication
	16	indirect data exchange
	17	indirect data exchange
10	18	direct data exchange
	19	block
	20	block
	21	block
	22	block
15	23	block
	24	block
	25	block
	26	block
	27	block
20	28	block
	29	block
	30	block
	31	block
	32	block
25	33	block
	34	block
	35	block
	36	block
	37	block
30	38	block
	39	block

CLAIMS

1. A method for authenticating of at least two agricultural devices coupled via a data bus prior to implementing data exchange therebetween, comprising the steps of:

5 coupling an authentication device and the at least two agricultural devices to the data bus;

utilizing the authentication device to authenticate each of the at least two agricultural devices coupled to the data bus automatically and independently;

10 upon successful authentication of the at least two agricultural devices, implementing direct data exchange or indirect data exchange between the successfully authenticated agricultural devices, automatically; and

upon unsuccessful authentication, blocking direct data exchange or indirect data exchange between the unsuccessfully authenticated agricultural devices.

15 2. The method according to claim 1, wherein the step of utilizing the authentication device to authenticate each of the at least two agricultural devices coupled to the data bus includes a step of verifying the authentication device via a particular agricultural device and a step of verifying the particular agricultural device via the authentication device.

20 3. The method according to claim 2, wherein the step of verifying the authentication device via a particular agricultural device includes:

transmitting, by the particular agricultural device, an identification number stored in a control device thereof and a random number determined by the control device thereof to the authentication device;

25 determining, by the authentication device, a first device key on the basis of the identification number transmitted by the particular agricultural device;

determining, by the authentication device, a second device key on the basis of the first device key and the random number transmitted by the particular agricultural device;

transmitting, by the authentication device, the second device key and a random number determined by the authentication device to the control device of the particular agricultural device; and

5 determining, by the particular agricultural device, a second device key on the basis of a first device key stored in the control device thereof and on the basis of a random number determined thereby and comparing the second device key determined thereby with the second device key determined and transmitted by the authentication device.

10 4. The method according to claim 3, wherein the step of verifying the particular agricultural device via the authentication device comprises the steps of:

determining, by the particular agricultural device, a third device key on the basis of the first device key stored in the control device thereof and on the basis of the random number transmitted by the authentication device and transmitting the
15 third device key to the authentication device; and

determining, by the authentication device, a third device key on the basis of the first device key determined thereby and on the basis of the random number determined thereby, and comparing the random number with the third device key determined and transmitted by the particular agricultural device.

20

5. The method according to claim 4, wherein upon successful verification of the authentication device and the particular agricultural device, the particular agricultural device is successfully authenticated.

25 6. The method according to claim 1, further comprising carrying out an indirect data exchange between successfully authenticated agricultural devices via the authentication device.

7. The method according to claim 1, further comprising a direct data exchange between successfully authenticated agricultural devices while bypassing the authentication device.

5 8. The method according to claim 7, wherein the bypassing of the authentication device includes:

determining, by the authentication device, a fourth device key for the first agricultural device on the basis of a further random number determined thereby and on the basis of a first device key determined thereby for a first agricultural device;

10 determining, by the authentication device, a combination key;

determining, by the authentication device, a system key for the first agricultural device on the basis of the first device key, on the basis of the fourth device key and the combination key;

15 transmitting, by the authentication device, the System key for the first agricultural device and the further random number to the first agricultural device;

determining, by the first agricultural device, a combination key on the basis of the system key and the further random number;

20 determining, by the authentication device, a fourth device key for the second agricultural device on the basis of a further random number determined thereby and on the basis of a first device key determined for a second agricultural device;

determining, by the authentication device, a system key for the second agricultural device on the basis of the first device key, on the basis of the fourth device key and on the basis of the combination key;

25 transmitting, by the authentication device, the system key together with the further random number to the second agricultural device;

determining, by the second agricultural device, the combination key on the basis of the system key and the further random number; and

using, by the first agricultural device and the second agricultural device, the same determined combination key for the encoded, direct data exchange.

9. An authentication device configured for authenticating at least two agricultural devices coupled via a data bus prior to implementing data exchange therebetween, utilizing a method comprising the steps of:

coupling an authentication device and the at least two agricultural devices to
5 the data bus;

utilizing the authentication device to authenticate each of the at least two agricultural devices coupled to the data bus automatically and independently;

upon successful authentication of the at least two agricultural devices,
implementing direct data exchange or indirect data exchange between the
10 successfully authenticated agricultural devices, automatically; and

upon unsuccessful authentication, blocking direct data exchange or indirect data exchange between the unsuccessfully authenticated agricultural devices.

10. A computer program product comprising program code means embodied in a
15 non-transitory computer readable medium for carrying out all steps of a method for authenticating of at least two agricultural devices coupled via a data bus prior to implementing data exchange therebetween, when the program code means is run on a computer or control device, the method comprising the steps of:

coupling an authentication device and the at least two agricultural devices to
20 the data bus;

utilizing the authentication device to authenticate each of the at least two agricultural devices coupled to the data bus automatically and independently;

upon successful authentication of the at least two agricultural devices,
implementing direct data exchange or indirect data exchange between the
25 successfully authenticated agricultural devices, automatically; and

upon unsuccessful authentication, blocking direct data exchange or indirect data exchange between the unsuccessfully authenticated agricultural devices.

1/3

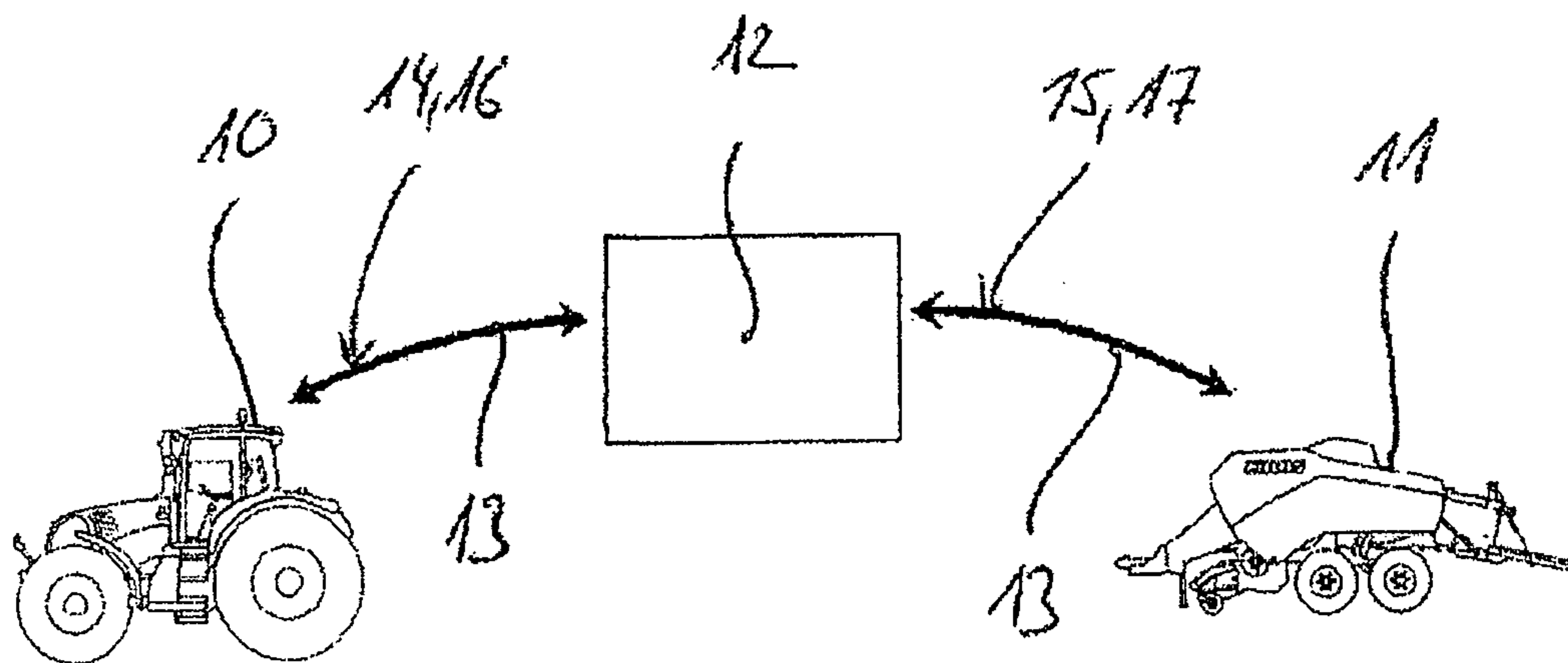


Fig. 1

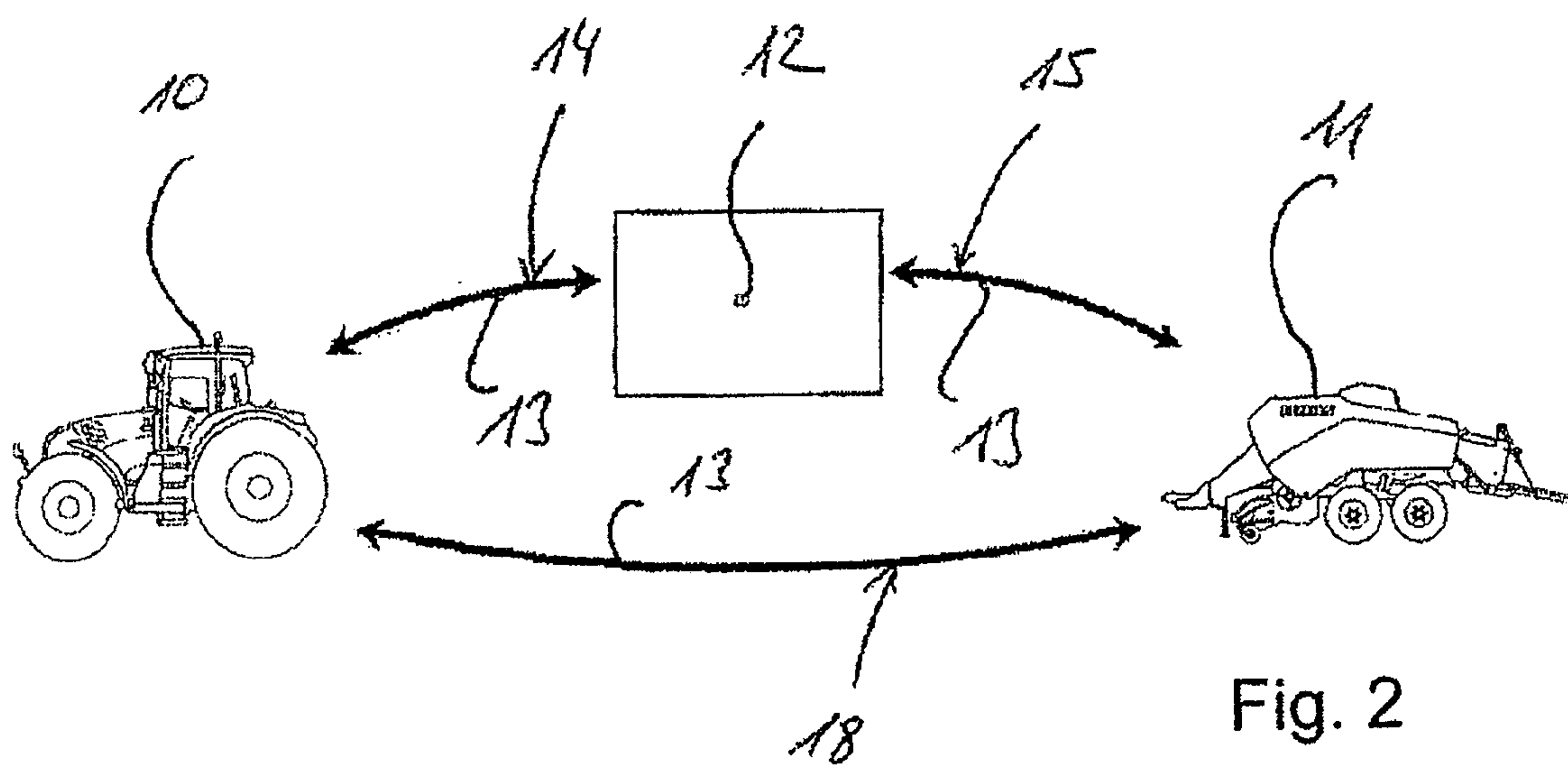


Fig. 2

2/3

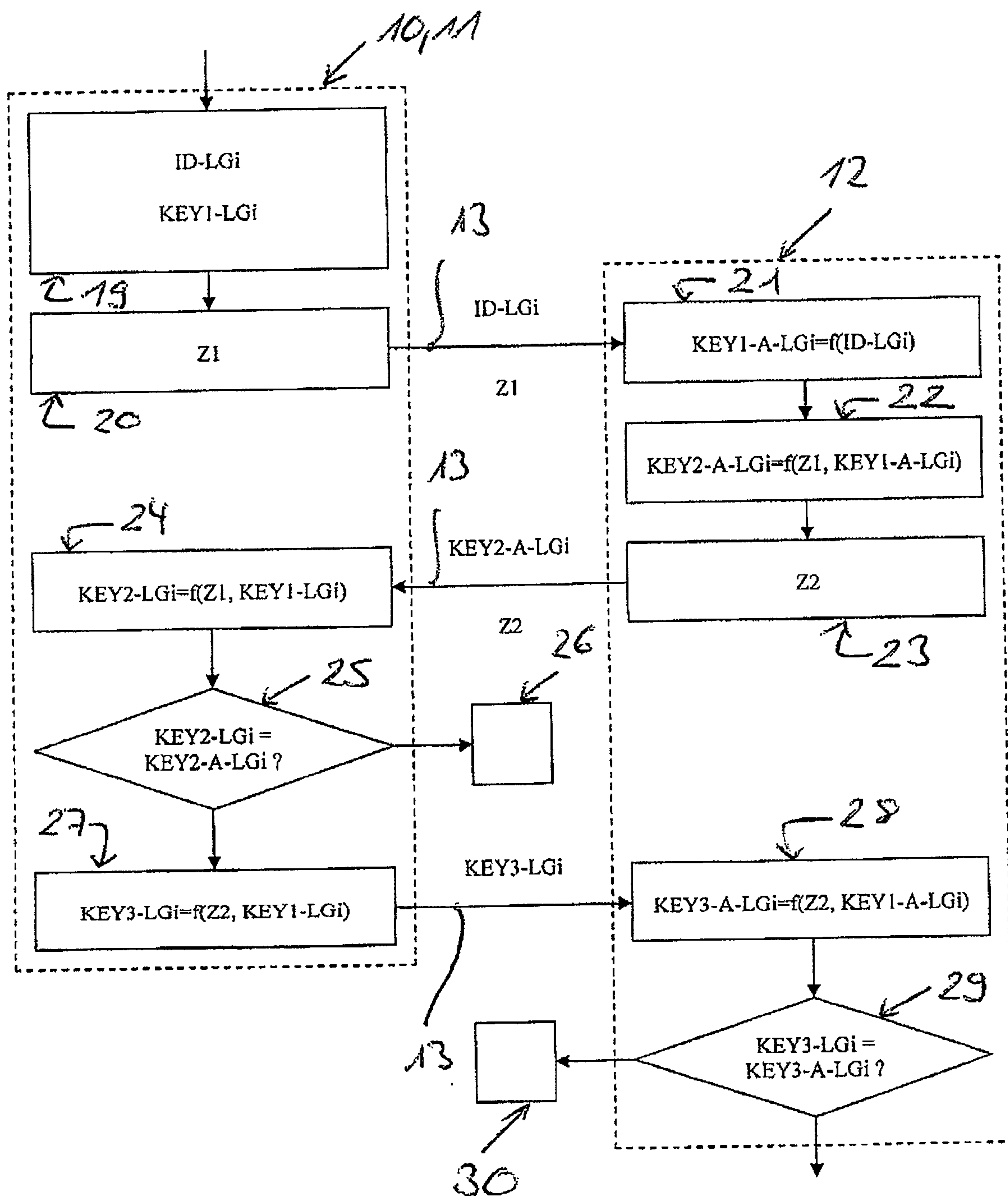


Fig. 3

3/3

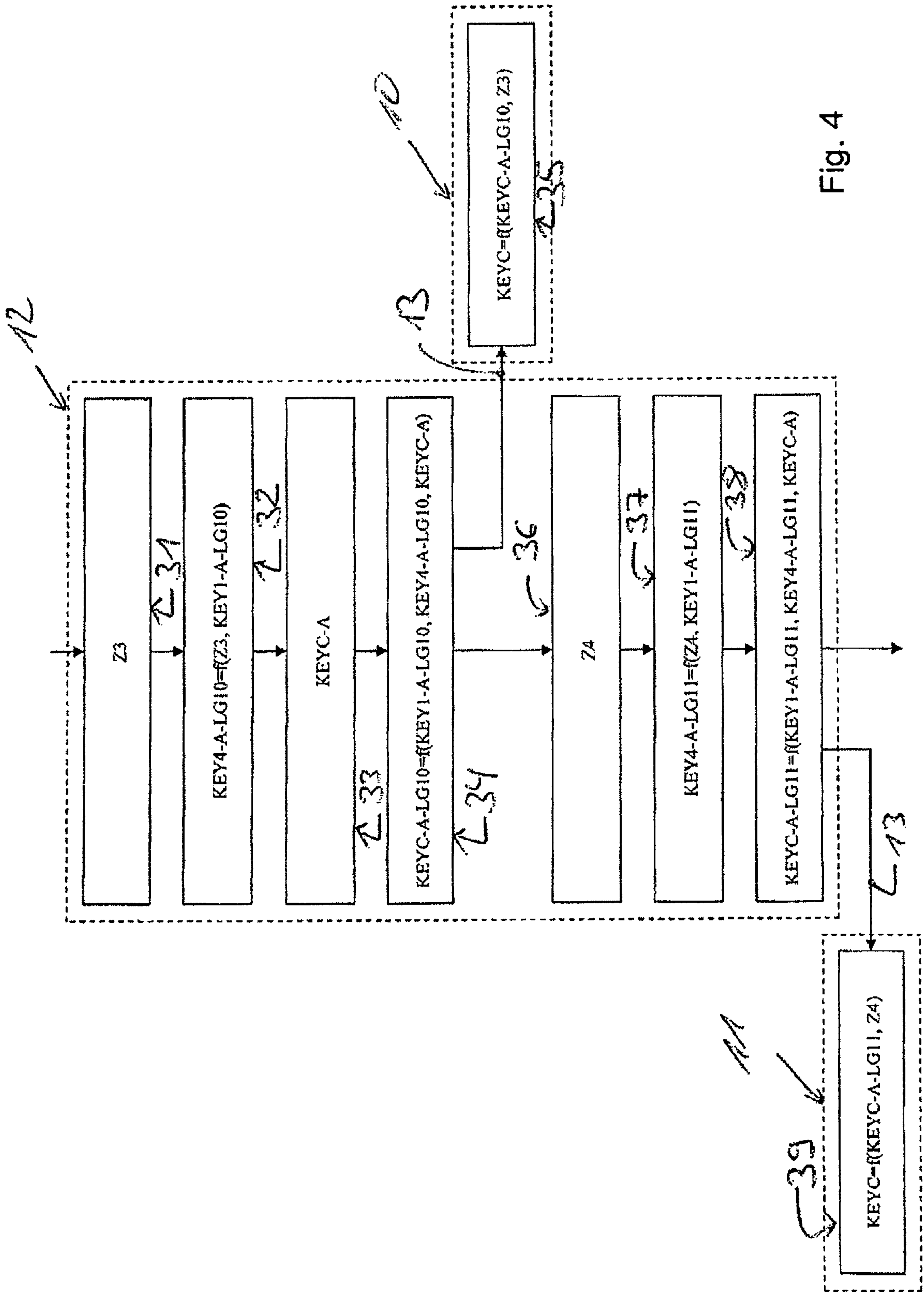


Fig. 4

